IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method of controlling content usage in a ~~personal~~ wireless communication device using a decryption key that is divided into at least first, second and third ~~a plurality of~~ key-shares, the method comprising ~~comprises~~:

pre-storing the third key-share in the wireless communication device;

providing the ~~personal~~ wireless communication device the [[a]] first key-share in response to a request for content; ~~and~~

verifying credit of a user of the ~~personal~~ wireless communication device; and

providing the ~~personal~~ wireless communication device the [[a]] second key-share when the credit is verified ~~confirmed; and~~,

wherein upon receipt of the content, the wireless communication device combines ~~combining~~ the first and second key-shares with the [[a]] third key-share that was pre-stored in the ~~personal~~ wireless communication device for use in decrypting the content, and

wherein the first, second and third key-shares are associated with the user and comprise a private decryption key of the user.

2. (Currently amended) The method as claimed in claim [[1]] 15 wherein the method includes:

monitoring usage of the content with [[a]] the security processor of the ~~personal~~ wireless communications device; and

purging at least one of the key-shares from the ~~personal~~ wireless communication device when the usage exceeds one of a set of measurement parameters stored in the personal communications device of the set.

3. (Currently amended) The method as claimed in claim 2 further comprising:

receiving the request for the content from the ~~personal~~ wireless communication device, the request identifying the content and the measurement parameters for the content; and

encrypting the content in the security server with an encryption key corresponding to the decryption key,

wherein the third key-share is pre-stored in the wireless communication device prior to encrypting the content.

4. (Currently Amended) The method as claimed in claim [[1] 15 further comprising ~~including~~:

in response to verification of the user's credit, receiving the content from a content server at ~~in a~~ the security server;

encrypting the content in the security server with ~~the~~ an encryption key corresponding to the decryption key; and

providing the encrypted content from the security server to the ~~personal~~ wireless communication device over a wireless communication link.

5. (Currently amended) The method as claimed in claim 4 wherein the content server and the security server communicate over a non-secure network, and

wherein the method includes the content server adding security to the content prior to providing the content to the security server.

6. (Currently amended) The method as claimed in claim [[1]] 4 wherein the providing the first of the key-shares is performed by [[a]] the security server over the wireless link in response to either the receipt of content at the security server or the encryption of the content by the security server in communication with the ~~personal~~ wireless communication device.

7. (Currently Amended) The method as claimed in claim 1 wherein the third ~~of the~~ key-shares is pre-stored in a subscriber identity module (SIM) associated with the user, ~~and~~

wherein a fourth of the key-shares is pre-stored in the ~~personal~~ wireless communication device and associated with a security processor of the ~~personal~~ wireless communication device, and

wherein the security processor combines the first, second, third and fourth key-shares to generate the decryption key and decrypt the encrypted content.

8. (Currently amended) The method as claimed in claim 1 wherein the verifying credit of the user and the providing the second of the key-shares to the ~~personal~~ wireless communication device are performed by a finance server in communication with the ~~personal~~ wireless communication device.

9. (Currently amended) The method as claimed in claim 1 further comprising generating the key-shares from the decryption key using a key-splitting technique ~~wherein the plurality of key-shares are Blakley-Shamir key-shares~~.

10. (Currently amended) The method as claimed in claim [[1]] 2 wherein the content comprises at least one of either video content or music content.

11. (Currently amended) The method as claimed in claim [[1]] 2 further comprising generating the [[a]] set of measuring parameters comprising at least one of a date-limit, a run-time limit, and an iteration limit, and

wherein the ~~personal~~ wireless communication device monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares when the usage exceeds one of the measurement parameters of the set.

12. (Currently amended) The method as claimed in claim 11 further comprising a content server defining the set of measurement parameters based on preferences of a content provider.

13. (Currently amended) The method as claimed in claim 11 wherein the date-limit defines an end calendar date for playing the content,

wherein the run-time limit defines a maximum amount of time for playing portions of the content, and

wherein the iteration limit defines a maximum number of times for playing the content or portions thereof.

14. (Currently amended) The method as claimed in claim 12 wherein the measurement parameters have an authentication code associated therewith, and

wherein a security processor of the ~~personal~~ wireless communication device purges at least one of the key-shares when the authentication code fails to authenticate.

15. (Currently amended) The method as claimed in claim 1 wherein the ~~personal~~ wireless communication device receives the first and second of the key-shares over a wireless communication link, and

wherein the third key-share is pre-stored in the wireless communication device prior to the user generating the request for the content and prior to a security server sending the content and the second key-share to the wireless communication device.

16. (Currently amended) A processing system for ~~use in~~ a ~~personal~~ wireless communication device, the processing system comprising:

a security processor portion to combine first, second and third ~~a plurality of~~ key-shares to generate a decryption key to ~~and~~ decrypt content for the processing system, the security processor portion including a monitor for usage of the content constructed and arranged to purge at least one of the key-shares when the usage exceeds a measurement parameter; and

a communications processor portion to receive decrypted content from the security processor portion and providing decrypted content for playing on the ~~personal~~ wireless communication device,

wherein the wireless communication device has the third key-share pre-stored therein and receives the first key-share and the second key-share over a wireless link in response to a request for content and a verification of a user's credit.

17. (Currently Amended) The processing system as claimed in claim 16 wherein the measurement parameters have an authentication code associated therewith, and

wherein the security processor portion purges at least one of the key-shares when the authentication code fails to authenticate.

18. (Currently amended) The processing system as claimed in claim 16 wherein the security processor portion has the third key-share pre-stored ~~a first of the key-shares stored~~ therein, retrieves a fourth key-share ~~second of the key-shares~~ from a subscriber identity module inserted into the ~~personal~~ wireless communication device, and receives the second key-share ~~a third of the key-shares~~ from a finance server when a user's credit is verified for use of the content,

wherein the security processor combines the first, second, third and fourth key-shares to decrypt the content.

19. (Currently amended) The processing system as claimed in claim 16 wherein the measurement parameters comprise at least one of a date-limit, a run-time limit, and an iteration limit, and

wherein the security processor portion monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares when the usage exceeds one of the measurement parameters ~~of the set~~.

20. (Currently amended) The processing system as claimed in claim 16 further comprising an applications processor portion to process applications running on the ~~personal~~ wireless communication device, and wherein the security processor portion, communications processor portion and applications processor portion are part of a processor area and fabricated on an application specific integrated circuit (ASIC).

21. (Currently amended) A ~~personal~~ wireless communication device comprising:

a processor area to pre-store first key-share therein;

a module receiving area to receive a subscriber identity module (SIM), the SIM having a second[[-]]key-share pre-stored therein; and

an RF interface to receive a third key-share and encrypted content over a wireless communication link in response to a request for content and verification of a user's credit,

wherein the processor area includes apparatus constructed and arranged to combine the first, second and third key-shares to decrypt the encrypted content and monitor playing of the decrypted content against measurement parameters[[.]],

wherein the first, second and third key-shares are associated with the user and comprise a private decryption key of the user, and

wherein the first key-share is pre-stored in the processor area and the second-key-share is pre-stored in the SIM prior to the device generating the request for the content and prior to a security server sending the content and the third-key-share to the wireless communication device.

22. (Currently amended) A ~~personal~~ wireless communication device as claimed in claim 21 wherein the measurement parameters have an authentication code associated therewith and wherein the processor area purges at least one of the key-shares when usage of the content exceeds a measurement parameter, or when the authentication code fails to authenticate.

23. (Currently amended) A ~~personal~~ wireless communication device as claimed in claim 21 wherein the processor area receives the third key-share from a finance server when a user is approved for use of the content in accordance with the measurement parameters.